ISSUE: 10 YEAR: 2016

University Information Security Office Newsletter

"People take things at face value on social media. Earnestness is the assumption."
— Mindy Kaling

From the ISO's Desk

October is National Cyber Security Awareness Month (NCSAM), conducted every October since 2004, this national public awareness campaign is intended to encourage everyone to protect their computers and our nation's critical cyber infrastructure. Cyber security requires vigilance 365 days per year. However, the Department of Homeland Security (DHS), the National Cyber Security Alliance (NCSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), the primary drivers of NCSAM, coordinate to shed a brighter light on what home users, schools, businesses and governments need to do in order to protect their computers, and data. This year, the LUC Information Security Staff will be hosting several small events on campus. Look for the "Security and Donuts" series at all campuses as well as the "Ask a security expert" table which will be located in the Information Commons. Posters will be distributed around campus as well. Don't forget about the awareness video series, Loyola Aware. Several modules have already been released and we continue to release a new video each month. This month's topic is "Social Networking" Please see page 2 for instructions on how to access the modules. If you would like to know more about our NCSAM activities, please check out Inside Loyola or go to our web page; https://www.luc.edu/uiso

Jim Pardonek
Information Security Officer

Social Networking Safely

SANS Securing the Human

Social networking websites are one of the most exciting technologies on the Internet. What makes these sites so powerful is how easy it is to share with others and to watch and learn what others are doing. However, you need to be aware that there are risks that come with these amazing capabilities. Here we will cover some simple steps you can take to protect yourself online.

Sharing Your Information

Social networking websites allow you to post and share a tremendous amount of information. Not only can you publish basic personal data, but also favorite songs and movies, personal photos and events in your life. The concern is that sharing all this information can harm you if you're not careful. Criminals and attackers look for highly personal information. They may be able to guess your passwords, impersonate you online or even steal your identity based on the details of your life you've shared. You should never post personal details, such as your birth date, home address or identification numbers, online. In addition, organizations hiring new employees or universities reviewing new students often do background checks on popular social networking sites, such as Facebook. To protect your future, do not post any embarrassing information or photos of yourself. If it is something you would not want your boss or family to see, you should simply not post it.

Also, be careful of what others share about you. Your friends may be posting confidential information or personal photos of you. Ask them to be considerate of your privacy and track what they are sharing about you. If they post anything you feel is inappropriate, ask them to remove the content or report it to the website's abuse department.

Trusting Others

Cyber attackers may attempt to fool you on social networking sites, just like they do in email or instant messaging. A common attack on sites like Facebook or Twitter is for a criminal to hack into a person's account and post messages pretending to be that person.

For example, your friend may post that he was just mugged while traveling overseas and lost all of his money and documentation. He desperately needs help and asks if you or anyone else can transfer some money right away. The problem is that your friend was never mugged. In fact, he was never even traveling. Instead, someone hacked into your friend's Facebook account and posted the fake message while pretending to be him. Just like with email, if you get suspicious messages on a social networking site from a friend, call them to confirm if they posted the message or not.

Third Party Apps and Games

Some social networking websites have additional third-party programs, such as games you can install. These programs are usually not developed or reviewed by the social networking website. Instead, other individuals or organizations develop them independently. Always be careful when using third-party programs, as they can potentially infect your computer or access your private information.

Continued Pg. 2

Security vs Privacy in Social Networking

LOYOLA UNIVERSITY CHICAGO
1870
AD MAJOREM DEI GLORIAM

What's the Difference?

When it comes to security issues on Social Networks, we are talking about hackers gaining unwarranted access to the actual code or protected language of the website. Privacy concerns the unauthorized access of the personal information of users and the control of one's personal information. This does not always entail a breach of security by a hacker, but the two often go hand-in-hand with one another.

Why is it Important?

Hackers are always looking for ways to breach the security of Social Networking platforms. Most of the time, they are attempting to access the personal information of users. But hackers are not the only interested parties in your personal information. Many large companies are trying to get inside the heads of their own consumers to hone their marketing chops.

The Big Value on Big Data

Your activity on social networking platforms creates data that these companies desperately crave. Anything from the pages you've liked, the music you've listened to this month, even the places where you have taken pictures recently; this all amounts to a consumer profile that allows companies to direct their marketing towards potential customers like yourself. And they're willing to put down a lot of money for this information.

Making Security and Privacy Work For You

Both security and privacy work in tandem to control the distribution of your personal information on social networking platforms.
Listed below are a few basic steps you can take to keep your account secure and personal information managed.

For Security...

- Keep your account passwords unique for individual sites. This practice ensures if one of your accounts is hacked, the other accounts will remain secure.
- Do not share your passwords with anyone.
- Always log out of your accounts after signing in from any machines that are not your own.

For Privacy…

- Manually manage your privacy settings on platforms such as Facebook and Instagram. By default, these settings are often set to publically share.
- Be mindful of whether the information you are sharing is really necessary, such as locations, political views, weekend plans, etc.

Social Networking Safely

Cont. from Pg. 1

Work Information

Do not post any confidential information about our organization on any websites. If you have any questions about what you can or cannot post about work, please ask your supervisor. In addition, be sure you are not using any of your work passwords for your social networking accounts; these personal accounts should have different passwords. This way, if any of the social networking websites you use are hacked, your work passwords are still secure.

Your Privacy Settings

Most social networking sites offer privacy controls. These are settings you can configure to determine who can and cannot access information on your page. The problem with most privacy controls is that they are complex; it is too easy to make mistakes. You may think your information is protected, only to discover that anyone can access it. Even once you figure out how the privacy options work and configure them accordingly, they often change.

If any of your friends' accounts become compromised, your information may be accessible by the attacker. The best way to protect yourself is to assume any information you post will eventually become public, regardless of the privacy controls you use. If you do not want your boss, coworkers or family members to find out about it, you shouldn't post it.

Loyola Aware

Our October awareness topic is " Social Networks".

Please visit: http://www.luc.edu/uiso/awareness/loyola_aware.shtml for further information.

If you have any questions in regrading to Loyola Aware, please contact the data security team by email (datasecurity@luc.edu) or call

University Information Security Office

Email: DataSecurity@luc.edu
Telephone: (773) 508-7373
Location: GC Room 230
Hours: M-F 8AM-5PM